PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/38

A1

(11) International Publication Number: WO 99/33309

(43) International Publication Date: 1 July 1999 (01.07.99)

(21) International Application Number: PCT/US98/27185

(22) International Filing Date: 21 December 1998 (21.12.98)

(30) Priority Data:
08/996,089 22 December 1997 (22.12.97) US

(71) Applicant: ERICSSON INC. [US/US]; 7001 Development Drive, P.O. Box 13969, Research Triangle Park, NC 27709 (US).

(72) Inventor: BALACHANDRAN, Shridharan; Apartment 191, 2815 Shiloh Road, Garland, TX 75044 (US).

(74) Agents: MOORE, Stanley, R. et al.; Jenkens & Gilchrist, P.C., Suite 3200, 1445 Ross Avenue, Dallas, TX 75202 (US).

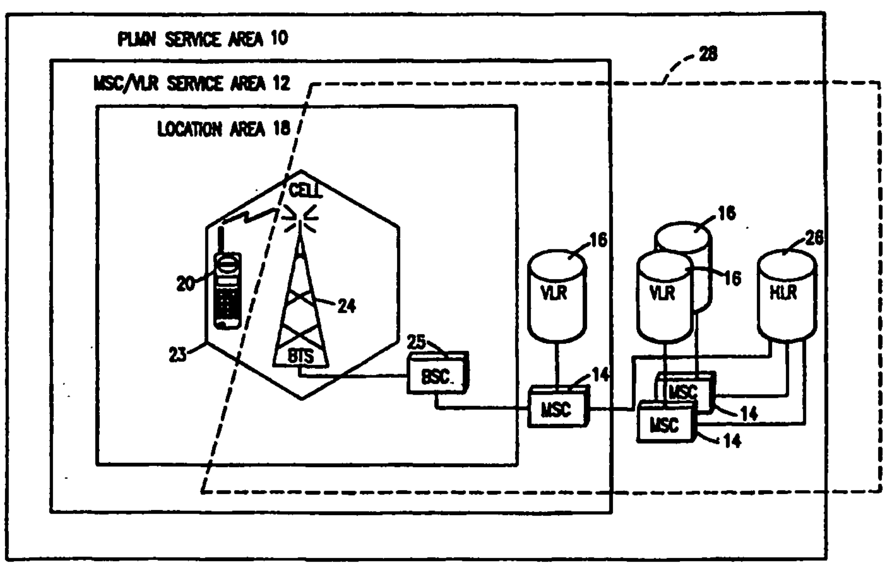
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SYSTEM AND METHOD FOR THE EARLY DETECTION OF CELLULAR TELEPHONE PIRACY

(57) Abstract



A method and system for early piracy detection in a cellular telecommunications network is disclosed. When in idle mode, a network subscriber Mobile Station (MS) transmits a Current Location Identifier message (CLID) on a pseudo–random basis. The CLID, which contains MS identifying information, is picked up by the network and relayed to the Mobile Switching Center (MSC) covering the area in which the MS is currently located. When it receives the CLID, the MSC generates an MS–CLID message containing the CLID and the identifier of the nodes through which it has passed, including that of the MSC itself. The MS–CLID message is then sent to the system Home Location Register (HLR), which compares the MS identification and location information to that stored in its database. The system generates a piracy alarm when the comparison determines that another caller using the same identity is currently active or that a call being initiated is originating from a location distant to the last reported location of the legitimate MS, allowing the system operator to take action prior to the loss of inordinate amounts of air time.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SYSTEM AND METHOD FOR THE EARLY DETECTION OF CELLULAR TELEPHONE PIRACY

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates to cellular telephone networks and, in particular, to a system and method for the early detection of cellular piracy, more particularly to a system and method where the system operator can take action to stop unauthorized system use upon activation of a piracy alarm signal.

Description of the Related Art

The evolution of wireless communication over the past century, since Guglielmo Marconi's 1897 demonstration of radio's ability to provide continuous contact with ships sailing the English Channel, has been remarkable. Since Marconi's discovery, new wireline and wireless communication methods, services and standards have been adopted by people throughout the world. This evolution has been accelerating, particularly over the last ten years, during which the mobile radio communications industry has grown by orders of magnitude, fueled by numerous technological advances that have made portable radio equipment smaller, cheaper and more reliable. The exponential growth of mobile telephony will continue to rise in the coming decades as well, as this wireless network interacts with and eventually overtakes the existing wireline networks.

In order to promote compatibility of the equipment and operations of various Public Land Mobile Networks (PLMN), air-interface standards have been developed and are currently being implemented. In North America, the most widely used standard protocol is the Advanced Mobile Phone System (AMPS), which is now being supplemented by a digital version (D-AMPS). Another such standard is the Global System for Mobile Communications (GSM), used throughout Europe and in some parts of the United States. In each standard, PLMN operators set up permanent equipment to cover a given geographical area and enlist mobile subscribers. The

subscriber is billed by the operator for cellular service, generally paying a base charge in addition to a variable charge based on the subscriber's use of the system.

Unfortunately, along with the popularity of cellular telephone has come cellular piracy. A pirate scans the air interface for cellular phones initiating a connection with the PLMN, exploiting initialization procedures. To begin a call, a cellular Mobile Station (MS) first transmits a signal over the air interface that includes unique MS identifying information. This identification information indicates that access to the cellular system is being requested by a system subscriber, and is used by the PLMN for, among other things, billing the subscriber for the call. An eavesdropping pirate who intercepts this initial transmission can then replicate the signal and construct a "clone," that is, an MS that transmits identical identification information.

When the clone thereafter initiates a call using the subscriber's identity, the PLMN cannot distinguish between the pirate caller and the legitimate subscriber; system access will be granted to both. The geographical location of the clone is no help in making any distinction, since the subscriber can "roam," that is, make and receive calls while located outside its home service area. Of course, the legitimate subscriber is billed for all the usage. Pirates often operate a single clone for approximately one month, after which time the subscriber will likely receive and protest an inordinately high cellular service bill. Although steps can then be taken to avoid further unauthorized use, the PLMN operator generally bears the cost of the calls already made by the clone, resulting in the loss of thousands of dollars of air-time revenue. This problem is most acute in PLMNs operating under the AMPS/D-AMPS protocols, which lack the techniques available, for example, as in the GSM environment.

At present, enforcement against pirates is difficult at best. Clones are quickly abandoned after short periods of high use, after which the pirate acquires another cloned identity. Accordingly, there exists a need for a way to detect clone use earlier so that unauthorized use may be stopped and an attempt made to track down the pirate before large amounts of air time are stolen.

SUMMARY OF THE INVENTION

To address that foregoing and other problems, the present invention proposes a system and method for initiating a clone alarm immediately when a potential piracy condition occurs. In a preferred embodiment, an idle Mobile Station (MS) belonging to a legitimate subscriber in a cellular telephone network, when not connected, transmits a Current Location Identifier message (CLID) on a pseudo-random basis. The CLID contains MS identification information. The CLID is picked up by the Base Transceiver Station (BTS) and transmitted through the Base Station Controller (BSC) to a Message Switching Center (MSC). The MSC assembles an MS Location Identifier message (MS-CLID) containing the CLID and identity of each node through which the CLID has passed. The MSC then transfers the MS-CLID to the system Home Location Register (HLR), which checks to see if an entity appearing identical to the CLID-transmitting MS is currently active. If so, a piracy condition exists and a clone alarm is transmitted to the system operator. Preferably, the frequency of the pseudo-random CLID transmissions can be varied by the system according to the current geographical location of the MS. More frequent transmissions could be made in areas known to have extensive piracy operations. In another embodiment, the identity check is performed in a separate authentication/privacy register (APR) to conserve HLR resources.

In yet another embodiment, whenever the HLR receives a registration from the MS or an MS-CLID, it updates its CLID database to reflect the new MS location information. Preferably, the location information stored in the HLR database will include the last-received MS-CLID. The HLR also initiates a transmission back to the MS so that the MS can store in non-volatile memory the MS-CLID stored in the HLR database. This stored MS-CLID is included by the MS when it next transmits a CLID. In this embodiment, when the HLR next receives an MS-CLID, then in addition to checking for active clones, it also verifies that the new MS-CLID contains within it the old MS-CLID previously returned to the MS. If not, a potential piracy condition exists because a clone is trying to emulate the MS by transmitting a CLID, and a clone alarm is transmitted to the system operator.

In yet another embodiment, the HLR also maintains information regarding the pseudo-random generation pattern that determines when an MS will transmit a CLID. Although an MS may fail to transmit a CLID at the next interval, for example because it is connected at the time, it is in this embodiment configured to transmit at an expected time. Upon receipt of an MS-CLID transmission, the HLR, in addition or as an alternative to other comparisons, verifies that the CLID was sent at an appropriate time. If not, a potential piracy condition exists and a clone alarm is transmitted to the system operator.

Upon receiving a clone alarm, the system operator can choose from several possible courses of action. For example, the operator could attempt to ascertain the suspected pirate's location, or could interrupt the suspected pirate's call to determine whether it is being placed by a legitimate subscriber. Short of investigating each alarm, the event could simply be noted and the suspected pirate's location recorded for future use. Tracking could then be initiated after a number of alarms have been received for the same MS. In any event, the system operator will have notice of a piracy situation long before a subscriber complains of an erroneous cellular telephone bill.

A more complete appreciation of the present invention and the scope thereof can be obtained from the accompanying drawings which are briefly described below, the following detailed description of the presently-preferred embodiments of the invention, and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and apparatus of the present invention may be obtained by reference to the following detailed description when taken in conjunction with the accompanying drawings, wherein:

FIGURE 1 is a block diagram of a telecommunications system according to the present invention;

FIGURE 2 is a block diagram of a telecommunications system illustrating the routing of a CLID/MS-CLID message according to the present invention;

FIGURE 3 is a flow chart illustrating how the system uses the MS-CLID in the piracy detection process according to one embodiment of the present invention;

FIGURE 4 is a block diagram illustrating the routing of CLID/MS-CLID and last reported location messages in accordance with the present invention; and

FIGURE 5 is a flow chart illustrating how the system uses the MS-CLID in the piracy detection process in accordance with an alternative embodiment of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

With reference to FIG. 1 of the drawings, there is illustrated Public Land Mobile Network (PLMN) 10, such as cellular network, which in turn is composed of a plurality of areas 12, each having a Mobile Switching Center (MSC) 14 and integrated Visitor Location Register (VLR) 16 therein. The MSC/VLR areas 12, in turn, include a plurality of Location Areas (LA) 18. An LA 18 is that part of a given MSC/VLR area 12 in which a Mobile Station (MS) 20 may move freely without having to send update location information to the Home Location Register (HLR) 26, described below. Preferably, the MSCs are connected to the HLR via a Signaling System #7 (SS7) network.

Each Location Area 18 is divided into a number of cells 23. MS 20 is the physical equipment, e.g., a car phone or other portable phone, used by mobile subscribers to communicate with the cellular network 10. A Base Transceiver Station (BTS) 24 is the physical equipment, illustrated for simplicity as a radio tower, that provides radio coverage to the geographical area of the cell 23 in which to handle radio traffic to and from the MS 20. One or more BTSs are controlled by a Base Station Controller (BSC) 25, and one or more BSCs may be governed by a single MSC 14.

With further reference to FIG. 1, the PLMN Service Area or cellular network 10 includes an HLR 26, which is a database maintaining all subscriber information, e.g., user profiles, current location and routing information, and other administrative information. The HLR 26 itself may be co-located with a given MSC 14, may be an integral part of an MSC 14, or may service multiple MSCs 14; the latter configuration being illustrated in FIG. 1. In accordance with the present invention, the BTS, BSC, MSCs, VLRs and HLR together make up a network security system 28.

The MS's current location stored in the HLR 26 database is in the first instance determined through a process called registration. In registration, MS 20 transmits a registration request message on a control channel to the cell-controlling BTS 24. The BTS 24 in turn directs the message through its associated BSC 25 to MSC 14 (updating VLR 16, if necessary, such as when MS 20 is roaming), and then to HLR 26. Registration typically occurs when MS 20 is powered-up, when it roams from one LA 18 to another, or at other predetermined times, such as when a call is placed. The MS 20 location information stored on the HLR 26 is used (in conjunction with VLR 16, if necessary), for example, when a call to the MS 20 is attempted.

As discussed, to steal air time from the cellular service provider, a pirate mimics the registration process when placing a call. By scanning the air interface, the pirate picks up a registration message and constructs a clone capable of sending an identical transmission. Since calls made from the clone will be indistinguishable from legitimate calls, both will be billed to the subscriber. The subscriber and the system operator will generally be unaware that cloning has occurred until a bill charging for call made by the clone is generated. Early piracy detection can be accomplished, however, by further cooperation between the MS 20 and network security system 28.

In a preferred embodiment of the present invention, during an idle period the MS 20 generates a signal, such as a Short Message Service (SMS)/page signal, called a Current Location Identification message (CLID). The CLID contains identification information unique to MS 20. With reference now to FIG. 2, there is shown a block diagram of a telecommunications system illustrating the routing of a CLID between the MS 20 and the HLR 26 according to the present invention. As with registration, the MS 20 first transmits the CLID over a control channel on the air interface to a

cell-controlling BTS 24. The BTS 24 then forwards the CLID to its BSC 25. From BSC 25, the CLID is sent to MSC 14. The MSC 14 determines the exact logical path back to MS 20, including the MSC 14 identifier, the VLR 16 identifier (if any) associated with MSC 14, the BSC identifier, and the BTS identifier. The MSC 14 then contacts HLR 26 and transmits a Mobile Station-Current Location Identifier message (MS-CLID), which includes the CLID and the aforementioned logical path identifiers. Preferably, the MS-CLID includes the CLID transmitted by the MS and the identifiers of the BTS, BSC, MSC, and (if applicable) VLR. It is not essential, however, that the MS-CLID comprise all of these elements, or that it exclude others, but it is preferable that the MS-CLID transmitted to the HLR 26 contain as precise location and signal-path information as is possible. Preferably, the CLID and MS-CLID transmissions are accomplished via a Signaling System #7 (SS7) Transaction Capabilities Application Part (TCAP) inquiry.

Reference is now made to FIG. 3, which is a flow chart illustrating how the HLR 26 uses the MS-CLID. As heretofore discussed, in accordance with the present invention the CLID, and hence the MS-CLID, contains within it a unique identifier associated with the MS 20 that originated the CLID transmission. The HLR 26 (shown in FIG. 2) contains the application that processes the MS-CLID signal. Upon receipt of the MS-CLID, step 301, the HLR 26, at step 305, initiates another TCAP inquiry to determine whether any other entity using the same unique MS identifier is active. Since the CLID is only transmitted by an idle MS, if any VLR 16 responds affirmatively, step 310, a clone alarm is generated by the HLR 26 at step 315. Alternately, activity status information could be continually updated by the VLRs 16 and stored in the HLR 26 database, in which case the simultaneous activity determination could be made without first making a TCAP inquiry (not shown). If, on the other hand, no VLR 16 responds affirmatively, step 320, then the HLR drops the MS-CLID message without generating an alarm, step 330.

In another embodiment, the HLR 26 determines at step 340 the logical path back to the clone, that is, the entity active when the MS-CLID was received. The time of the alarm, the MS 20 location, and the clone location are then recorded for future reference, step 350.

Although the CLID can be sent any time the MS 20 is idle, it is preferably initiated on a pseudo-random basis. This prevents a pirate from evading detection simply by placing calls during intervals when no CLID transmission is expected. The frequency of the pseudo-random transmissions is determined by an algorithm and seed resident in the MS 20. As these are never transmitted by the MS, it is not possible for a pirate to accurately predict the time of the next CLID transmission.

In a particularly preferred embodiment (not shown in FIG. 3), when the HLR 26 is notified that the MS is operating in an area with high piracy activity, as determined by the system operator based on past experience, the HLR 26 requests that the MSC 14 of the area in which MS 20 is currently operating generate a new seed and transmit it to the MS 20 The new seed, in combination with the algorithm resident on the MS 20, results in CLID transmissions occurring at more frequent intervals. When the MS leaves the area, CLID frequency is reduced in the same way.

In yet another embodiment (not shown in FIG. 3), a powered-down MS 20 will be automatically powered-up at the appropriate time to send a CLID message and then powered down again to conserve battery power. This feature could be manually disabled when CLID transmission should not occur, such as during a plane flight.

In yet another embodiment, the simultaneous activity check is not performed by the HLR 26 itself, but by a separate Authentication/Privacy Register (APR) 27 (shown in FIG. 2), which has access to the HLR 26 database. In this embodiment, the HLR resources are not diverted to this separate operation, except for acting as an intermediary message transfer node.

The amount of information contained in the piracy alarm message, or that is recorded, varies at the discretion of the system operator. It is preferable that the operator be notified of the cause of the clone alarm, and of the location of the clone as near as can be determined. Upon receiving a piracy alarm, the system operator could attempt to more precisely identify the clone's location by standard techniques, such as signal loop-back time/triangulation.

Reference is now made to FIG. 4, which is a block diagram illustrating another embodiment of the present invention. In this embodiment, increased protection is obtained, although at a higher burden on system resources. Referred to here as

"heavyweight" protection, this embodiment provides increased piracy detection in instances when the clone is not active simultaneously with a CLID transmission. To achieve this result, MS 20 has a non-volatile memory address (LM) 21 where the last calculated MS-CLID is stored. In heavyweight configuration, the CLID and MS-CLID are transmitted as aforedescribed in reference to FIG. 2, but in addition, the MS-CLID, preferably including the identifier of the BST, the BSC, and the MSC, along the path traveled by the CLID or registration message, is returned via the same path to MS 20 where it is stored in the LM 21. Generally, when LM 21 stores an MS-CLID received by MS 20, any previously stored information is deleted. It is foreseen, however, that multiple MS-CLIDs could be stored and applied to providing additional protection in accordance with the present invention. Whenever a CLID is generated by MS 20, it includes the last-received MS-CLID stored in LM 21 (and, if desired, additional historical information).

Reference is now made to FIG. 5, which is a flow chart illustrating the heavyweight operation of HLR 26 in conjunction with an associated APR 27. In this embodiment, when the HLR 26 receives an MS-CLID (step 301), it generates a TCAP query containing the MS-CLID and transmits it to APR 27 (step 500). The APR 27 then performs a number of checks (which are hereinafter described in a preferred sequence, but which can be performed in any order without deviating from the spirit of the invention).

First, the APR 27 performs the aforementioned simultaneous activity check. Upon receipt of an MS-CLID, APR 27 determines at step 505 whether any other entity using the same unique MS identifier is active. For the purposes of this embodiment, it is unimportant whether information concerning MS activity status is continually updated in the APR 27 (or HLR 26) database, or whether a separate query must be made to determine the information whenever an MS-CLID is received. As aforedescribed with reference to FIG. 3, if any VLR 16 responds affirmatively, step 510, a piracy condition exists and a clone alarm is generated at step 315. If, on the other hand, no affirmative response is received, step 320, then the other checks are nonetheless performed, preferably beginning with the timing check (step 530).

The APR 27, which has stored in its database the pseudo-random CLID interval algorithm and seed used by MS 20, verifies at step 530 that the CLID was generated at an expected time. Although a pirate may intercept and emulate a CLID, it will not have the algorithm and seed possessed by MS 20 and APR 27. Any CLID transmitted by a clone will therefore almost certainly occur at the wrong interval. If APR 27 determines at step 530 that this has occurred (step 535), a piracy condition exists and a clone alarm is generated (step 315).

In addition, because the previously received MS-CLID was both stored and returned to the MS 20, the APR 27 database (or, alternatively the HLR 26 database) and the LM 21 both hold in storage the same MS-CLID. When the MS 20 next transmits a CLID message, it includes this previous location information ("old MS-CLID"), which is in turn included in the "new MS-CLID" calculated by MSC 14 and transmitted to HLR 26 and APR 27. If step 530 confirms that the CLID was generated at an expected interval (step 540), this old MS-CLID, now contained in the newly received MS-CLID, is compared in step 550 to the old MS-CLID stored in the HLR 26 or APR 27 database. If the old MS-CLIDs do not match, step 555, a possible piracy situation exists or has occurred and a piracy alarm is sent to the system operator, step 315. Of course, if no previous MS-CLID was stored in a system database and transmitted to MS 20 for storage in LM 21, then a "match" will still occur. If a match occurs, step 560, the HLR 26 or APR 27 again updates its database to reflect the newly received MS-CLID, step 565, and notifies the MSC 14 (step 570), which transmits the new MS-CLID to the MS 20, where it replaces the previously stored information in LM 21 (step 575).

Although a specific process is illustrated in FIG. 5, it should be noted that it is not critical to the invention how the data storage, data processing, or alarm functions are allocated between the HLR 26 and the APR 27. Even in the heavyweight embodiment, all functions could be performed by the HLR 26 and it is not necessary in that case that an APR 27 is present. As with the aforedescribed lightweight mode, if the HLR 26 (or APR 27) is updated when an MS 20 becomes active or inactive, a separate TCAP query to determine this status (upon receipt of an MS-CLID) can be eliminated. Also, as aforedescribed with reference to FIG. 3, if desired, the system

could also or in the alternative determine the clone's location, step 340, and generate a clone report (step 350).

Although an embodiment of the method and apparatus of the present invention has been illustrated in the accompanying drawings and described in the foregoing detailed description, it will be understood that the invention is not limited to the embodiment disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

The previous description is of a preferred embodiment for implementing the scope of the invention should not necessarily be limited by this description. The scope of the present invention is instead defined by the following claims.

WHAT IS CLAIMED IS:

1. A method for detecting piracy of a mobile station within a cellular telecommunications system, said method comprising the steps of:

maintaining, within a database of said telecommunications system, an activity flag associated with said mobile station, said activity flag being set when said mobile station is active;

transmitting, by said mobile station, an identification signal a plurality of times while said mobile station is idle;

determining, after at least one of said identification signal transmissions, whether said activity flag for said idle mobile station is active; and

generating an alarm signal if said activity flag for said idle mobile station is active.

2. The method of claim 1, wherein said identification signal is transmitted by said idle mobile station at pseudo-randomly spaced intervals.

3. The method of claim 2, wherein said pseudo-random intervals are determined using an algorithm that is stored in both said mobile station and said database, and further comprising the steps of:

determining, after at least one of said identification signal transmissions, whether said at least one identification signal transmission occurred at a time predictable by said algorithm; and

generating an alarm signal if said at least one identification signal transmission was not sent at a time predictable by said algorithm.

4. The method of claim 2, further comprising the step of varying the frequency of said pseudo-random transmissions by a control signal sent to said mobile station.

5. The method of claim 4, wherein said varying step varies said frequency of said pseudo-random transmissions based on the areas in which said mobile station had been recently operating.

6. The method of claim 1, further comprising the steps of:

maintaining, within a database of said telecommunications system, a last-reported location of said mobile station;

determining, after said at least one identification signal transmission, a current location of said mobile station within said telecommunicating system;

comparing said current location of said mobile station after said identification signal transmission to said last-reported location; and

generating an alarm signal if said current location of said mobile station is different from said last reported location.

7. The method of claim 1, further comprising the steps of:

determining, after said at least one identification signal transmission, the identification signal path, wherein said identification signal path includes an identifier corresponding to at least one of the nodes of said telecommunication system through which said identification signal has been most recently transmitted;

maintaining, within a database of said telecommunications system, said identification signal path;

updating, after said comparison step, said last reported location of said mobile station within said location database to the current location;

transmitting, to said mobile station, said identification signal path;

storing, within a memory of said mobile station, said identification signal path as it is received;

transmitting, from said mobile station, a second identification signal, wherein said second identification signal includes said updated identification signal path last received by said mobile station;

comparing said identification signal path within said second identification signal to said identification path in said database of said telecommunications system; and

generating an alarm signal if said identification signal path within said second identification signal is different from said identification signal path in said database of said telecommunications network.

8. The method of claim 1, wherein said database of said telecommunications system is located within a home location register of said telecommunications system.

9 The method of claim 1, wherein said determining step is performed within an authentication register in communication with the home location register of said telecommunications network.

10. The method of claim 1, wherein said transmitting step is performed automatically.

11. The method of claim 10, wherein said mobile station, if in a powered-off condition at the time said identification signal is scheduled for transmission, automatically powers-on for a period at least long enough for said transmission to occur.

12. The method of claim 1, wherein said activity flag indicates whether the mobile station is active based on a query to visitor location registers in communication with said telecommunications system.

13. The method of claim 12, wherein said query is made after at least one of said identification signal transmissions.

14. The method of claim 1, wherein said activity flag is set based on a notification provided by visitor location registers when said mobile station becomes voice-active or inactive.

15. The method of claim 1, additionally comprising the step of determining a specific area in which a suspect clone is operating.

16. The method of claim 15, wherein said suspected operating area is determined by a signal loop-back time triangulation process.

17. The method of claim 1, wherein said alarm signal causes a piracy report to be generated.

18. A method for detecting piracy in a telecommunications system, said method comprising the steps of:

maintaining, within a home location register, a location database containing a plurality of locations of a corresponding plurality of active mobile stations associated with the telecommunications system;

transmitting, from a given one of said mobile stations, a current location identifier, said current location identifier corresponding to said given mobile station;

relaying said current location identifier of said given mobile station to said home location register;

determining, within said home location register upon receipt of said current location identifier, whether an active mobile station identifier, for at least one of said locations in said location database of said active mobile stations, matches said current location identifier; and

generating an alarm if, in said step of determining, said current location identifier matches said active mobile station identifier.

19. The method of claim 18, further comprising the steps of:

determining the location of said given mobile station transmitting said current location identifier;

updating said location database in the home location register to said current location identifier location;

transmitting said current location identifier location to said given mobile station, said given mobile station storing said current location identifier location in a memory therein;

transmitting from said given mobile station, a second current location identifier, said second current location identifier including said stored current location identifier;

comparing said stored current location identifier in said second current location identifier to said current location identifier for said given mobile station in said location database; and

generating said alarm if the stored current location identifier within said second current location identification does not match said current location identifier for said given mobile station in said location database of said home location register.

20. The method of claim 19, further comprising the step of determining the location of a suspected clone whenever said alarm is generated.

21. The method of claim 20, wherein said alarm caused a piracy report to be generated.

22. The method of claim 18, further comprising the steps of:

counting the number of current location identifiers transmitted by said given mobile station within a predetermined period; and

alerting the system operator if the number of transmissions counted in said counting step exceeds a predetermined threshold.

23. A cellular telecommunications system for detecting piracy of a mobile station, said system comprising:

a home location register having a location database containing the last reported location of a plurality of mobile stations associated with said home location register;

a signal generator in at least one of said mobile stations for sending respective current location messages to said home location register;

determining means for determining if an identifier corresponding to a given one of said mobile stations matches the identifier corresponding to at least one other active mobile station sending said respective current location messages; and

an alarm generator for generating an alarm if said given one mobile station identifier matches said other active mobile station identifier.

24. The system of claim 23, wherein said home location register determines the current location of said given mobile station and transmits said current location to said mobile station, and further comprising a storage location in said mobile station for storing location information sent to it from said home location register.

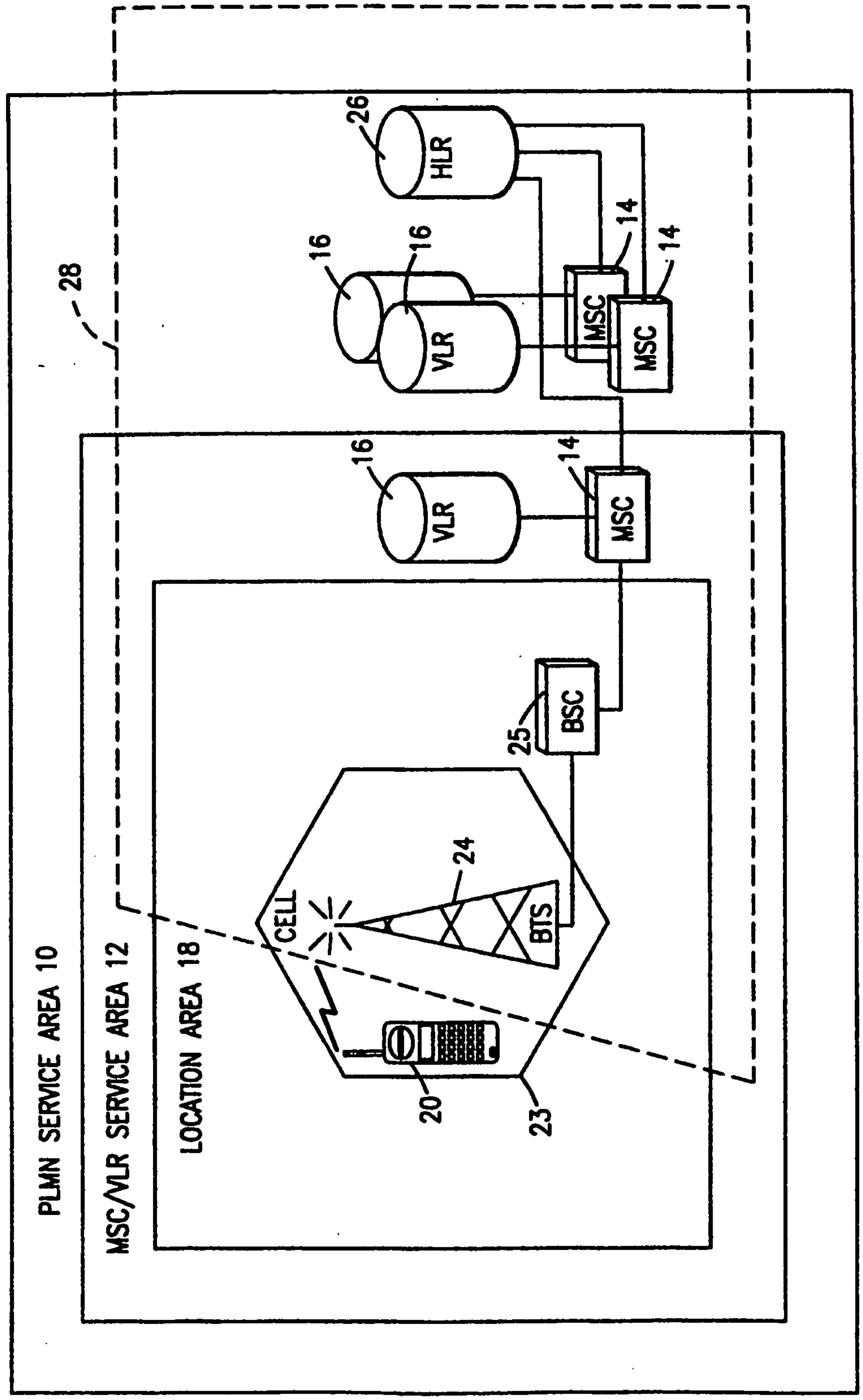

PLMN SERVICE AREA 10
MSC/VLR SERVICE AREA 12
LOCATION AREA 18
CELL
BTS
BSC
MSC
MSC
MSC
VLR
VLR
HLR
28
26
16
16
16
14
14
14
25
24
20
23

FIG. 1

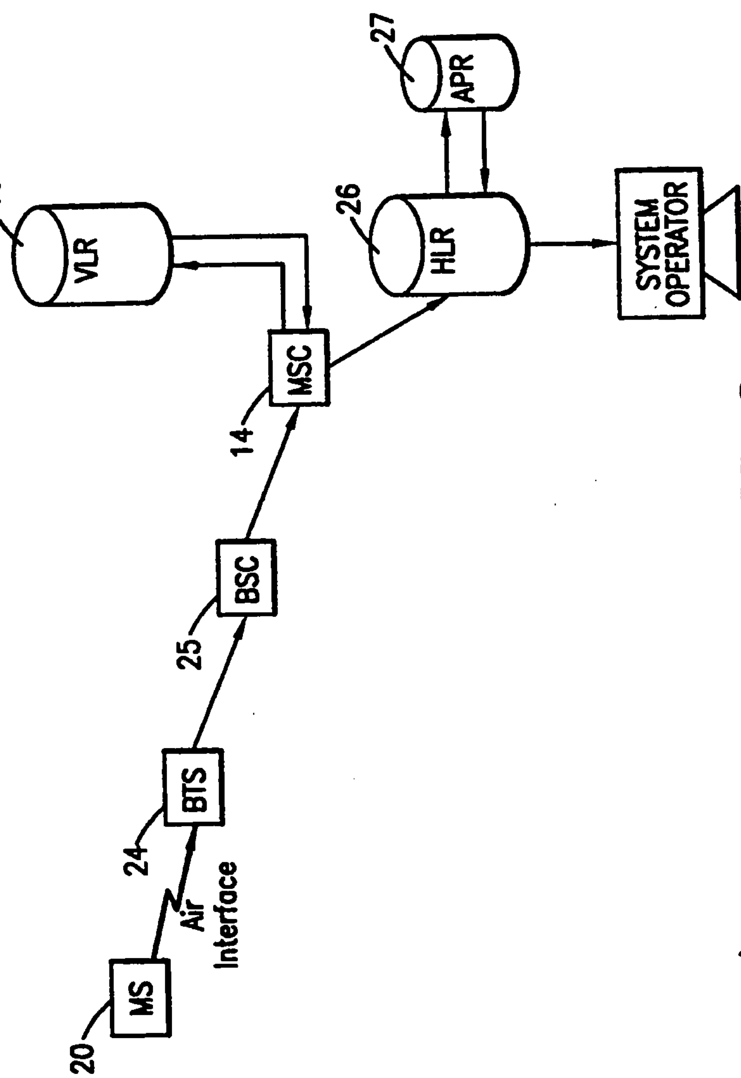

20
MS
Air
Interface
24
BTS
25
BSC
14
MSC
16
VLR
26
HLR
27
APR
SYSTEM
OPERATOR

FIG. 2

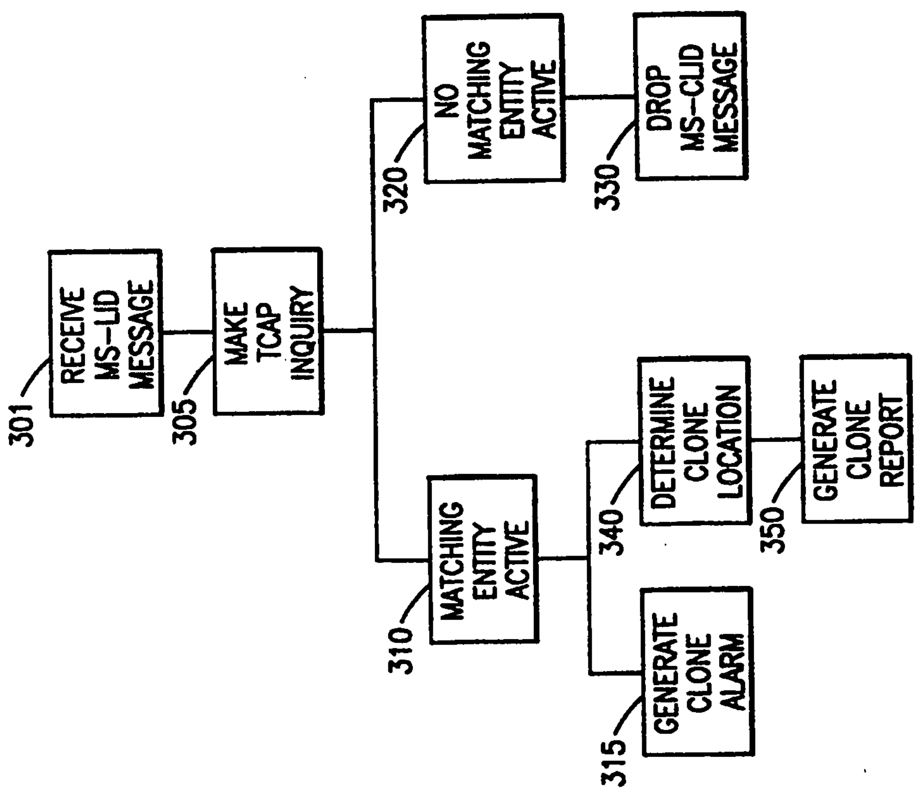

301
RECEIVE MS-LID MESSAGE
305
MAKE TCAP INQUIRY
310
MATCHING ENTITY ACTIVE
315
GENERATE CLONE ALARM
340
DETERMINE CLONE LOCATION
350
GENERATE CLONE REPORT
320
NO MATCHING ENTITY ACTIVE
330
DROP MS-CLID MESSAGE

FIG. 3

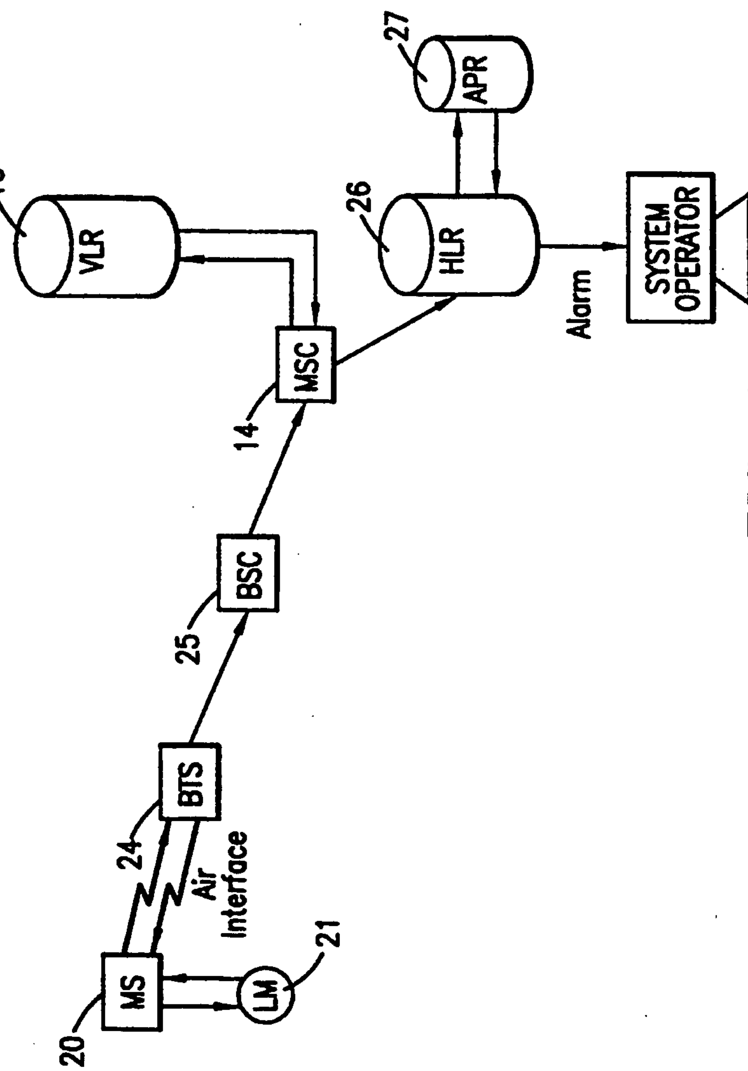

16
VLR
14
MSC
25
BSC
24
BTS
Air
Interface
20
MS
LM
21
26
HLR
27
APR
Alarm
SYSTEM
OPERATOR

FIG. 4

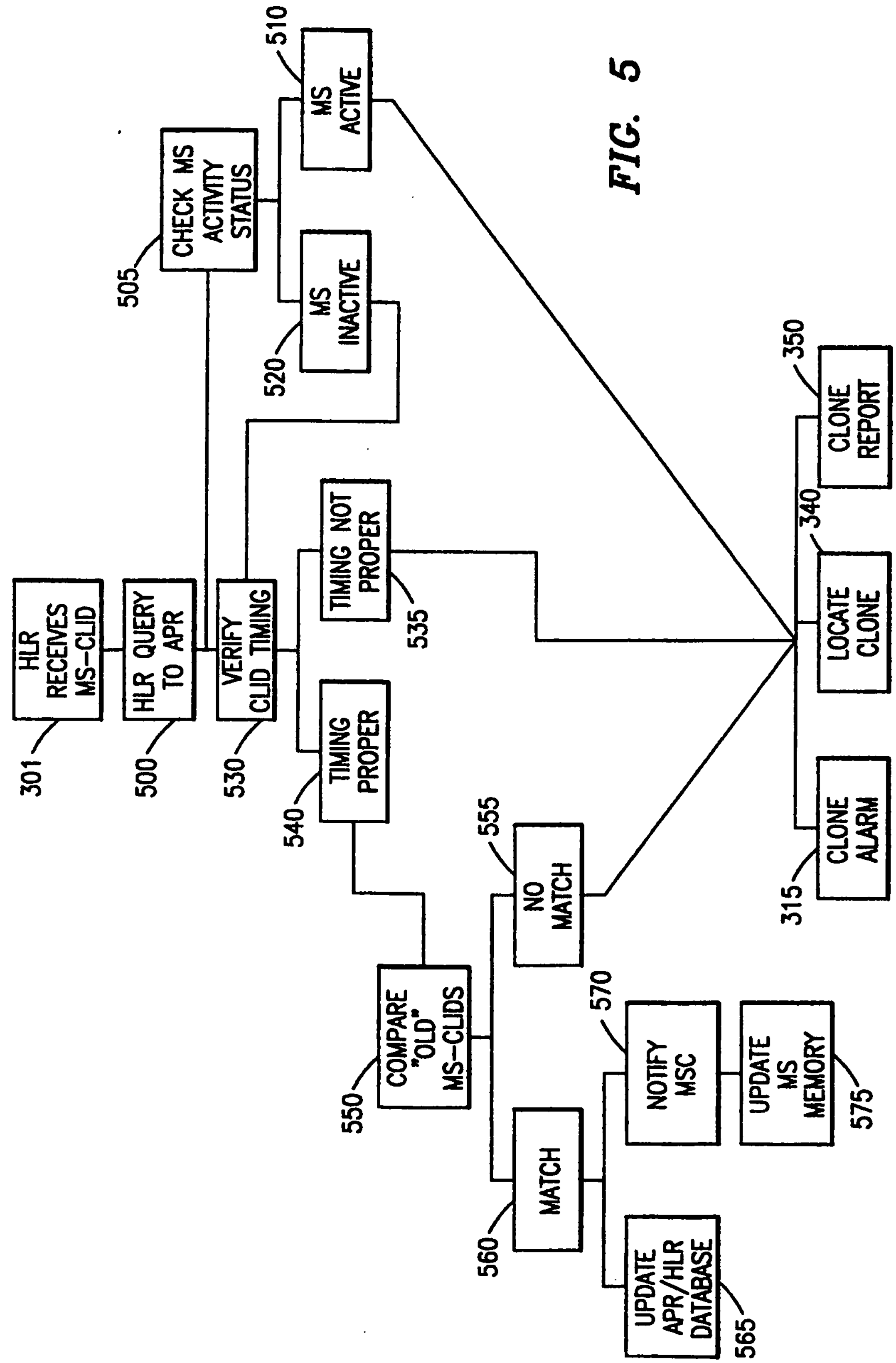

301
HLR RECEIVES MS-CLID
500
HLR QUERY TO APR
530
VERIFY CLID TIMING
505
CHECK MS ACTIVITY STATUS
510
MS ACTIVE
520
MS INACTIVE
535
TIMING NOT PROPER
540
TIMING PROPER
550
COMPARE "OLD" MS-CLIDS
555
NO MATCH
560
MATCH
565
UPDATE APR/HLR DATABASE
570
NOTIFY MSC
575
UPDATE MS MEMORY
315
CLONE ALARM
340
LOCATE CLONE
350
CLONE REPORT

FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/27185

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 15643 A (ERICSSON TELEFON AB L M) 23 May 1996	1,6,8, 10,12, 13, 15-18,23
	see page 4, line 1 - page 5, line 6 see page 11, line 33 - page 12, line 13 see page 14, line 1 - page 16, line 29 see page 27, line 34 - page 33, line 14 see page 33, line 29 - page 34, line 8	
A	see page 36, line 24 - page 39, line 2	2,3

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 April 1999	28/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Baas, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inti Jonal Application No
PCT/US 98/27185

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	PATEL S: "Location, identity and wireless fraud detection" 1997 IEEE INTERNATIONAL CONFERENCE ON PERSONAL WIRELESS COMMUNICATIONS (CAT. NO.97TH8338), 1997 IEEE INTERNATIONAL CONFERENCE ON PERSONAL WIRELESS COMMUNICATIONS CONFERENCE PROCEEDINGS, MUMBAI, INDIA, 17-19 DEC. 1997, pages 515-521, XP002099196 ISBN 0-7803-4298-4, 1997, New York, NY, USA, IEEE, USA see page 516, right-hand column, line 28 - page 518, left-hand column, line 5 see page 518, right-hand column, line 35 - page 519, right-hand column, line 41	1,6,8, 10-13, 18,23
A	see page 520, right-hand column, line 29 - line 49	2,3
A	EP 0 544 449 A (AMERICAN TELEPHONE & TELEGRAPH) 2 June 1993 see page 13, column 39 - column 57	1,18,23
A	WO 93 09640 A (ELECTRONIC DATA SYST CORP) 13 May 1993 see page 17, line 13 - page 20, line 24; figure 4	1,18,23
A	PATENT ABSTRACTS OF JAPAN vol. 014, no. 533 (E-1005), 22 November 1990 & JP 02 224425 A (NIPPON TELEGR & TELEPH CORP), 6 September 1990 see abstract	19,24

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/27185

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9615643 A	23-05-1996	US 5734977 A	31-03-1998
		AU 3942395 A	06-06-1996
		BR 9509723 A	21-10-1997
		CA 2204992 A	23-05-1996
		SE 9701723 A	08-07-1997
EP 0544449 A	02-06-1993	AT 149780 T	15-03-1997
		CA 2078195 A	28-05-1993
		DE 69217845 D	10-04-1997
		DE 69217845 T	26-06-1997
		ES 2098459 T	01-05-1997
		FI 925384 A	28-05-1993
		JP 2552065 B	06-11-1996
		JP 6069879 A	11-03-1994
		US 5309501 A	03-05-1994
WO 9309640 A	13-05-1993	DE 69227122 D	29-10-1998
		DE 69227122 T	25-03-1999
		EP 0611513 A	24-08-1994
		JP 7500955 T	26-01-1995
		US 5335265 A	02-08-1994